International Journal of Engineering Research
Volume No.3, Issue No.4, pp : 221-225

ISSN:2319-6890)(online),2347-5013(print)
01 April 2014

Literature review: Cloud Computing –Security Issues, Solution and Technologies

Rajani Sharma, Rajender Kumar Trivedi
Graphic Era University
rajanisharma65@gmail.com,engineertrivedi@gmail.com

Abstract— Cloud computing has grabbed the spotlight in the year 2013 at a conference in San Francisco, with vendors providing plenty of products and services that equip IT with controls to bring order to cloud chaos. Cloud computing trend is increasing rapidly so to make cloud computing more popular the very first step for the organization is to identify exact area where the cloud related threats lie. At an unusual pace, cloud computing has transformed business and government. And this created new security challenges. The development of the cloud service model provide business – supporting technology in a more efficient way than ever before .the shift from server to service based technology brought a drastic change in computing technology. However these developments have created new security vulnerabilities, including security issues whose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and security solutions.

*Keywords—**Cloud Computing, Deployment Models, Threats, Technologies, Security Issues, Service Models.***

I. Introduction

Cloud computing is set of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. These new innovative, technical and pricing opportunities bring changes in the way business operated. Cloud computing is the matchless computing technology. Cloud computing is a new label to an old idea. Cloud computing is a collection of resources and serviced provided by cloud service provider through internet. Cloud services are distributed from data canters sited all over the world. Cloud computing makes possible for its users to use the virtual resources via internet as per requirements. Cloud computing grabbed the spotlight in few years. General example of cloud services are Google Engine, Oracle Cloud, Office 365. As the cloud computing is growing rapidly this also leads to severe security concerns. Lack of security is the only barrier in wide adoption of cloud computing. The rapid growth of cloud computing has brought many security challenges for users and providers.

II. Cloud Service Models

Cloud Software-as-a-Service: Software –as-a-Service is a software distribution scheme which gives right to access the software and its functions remotely as a web-based service. Software-as-a-Service permits organizations to get into business functionality a very low cost normally less than paying for licensed applications in view of the fact that SaaS charges are built on a monthly fee. As so the software is hosted remotely users do not require to pay for additional hardware. Software-as-a-Service eliminates the all possibilities for organizations to handle the installation, set-up, daily preservation and maintenance. Cloud Platform-as-a-Service: the capability provided to the users to deploy onto the cloud infrastructure. PaaS model, cloud suppliers brings a computing platform, naturally comprising Operating System, Programming Language execution environment, database and wed servers. Application developers can develop and run their software results on cloud platform with no cost and difficulty of acquiring and handling of the main hardware and software films, for examples Oracle cloud platform-as-a-service, Oracle provides the Database as platform. And other example is windows azure. In other means Platform-as-a-Service is the facility to offer to the users to deploy user-designed or obtained applications on the cloud infrastructure. PaaS can largely be characterized as application development environments proposed as a 'Service' via the cloud supplier. Users uses these platforms which is being normally have Integrated Development Environment (IDE), so as it comprises the editor, compiler, build/execute and deploy features to develop their applications. And users deploy their applications on the infrastructure provided by the cloud supplier.

Cloud Infrastructure-as-a-Service: The cloud infrastructure such as hardware, servers, routers, storage, and other networking modules all are granted by the IaaS supplier. The end user takes on these offered services based on their requirements and pay for what they have used. The end user is capable of deploy and run any software, which comprise Operation Systems, applications. The end user does not supervise or monitor the core cloud infrastructure, but has hold over the operation systems and deployed application. At this juncture the end user needs to experience the resource requirements for the precise application to make use of IaaS properly. Flexibility and scaling are the liabilities of the end user, not the supplier. Moreover IaaS is small task performing - it-yourself information hub so as you would require to form the means (server, storage) and make the task completed. Waiting right away, small end users did not have the investment to make a purchase of immense computing resources and to make sure that they had the space they wanted to manage unpredicted spikes during load. Amazon Elastic Compute Cloud (Amazon EC2) is an infrastructure –as-a-Service model that facilitates scalable compute volume, on demand, in the cloud. It actually allows end users to leverage Amazon's huge infrastructure with no up-front investments. Amazon EC2 decreases the clock needed to get hold of and boot latest server instances and permit users to immediately scale space – equally up and down as their computing needs vary.

III. Cloud Deployment Models

Public Cloud-A cloud is to be entitled as public cloud when the services (like applications, storage) are being provided over network that are available publically, anyone can access it.

Public cloud's benefits may be taken as on a pay per usage mode or other purchasing schemes.

Private Cloud – A private cloud is an infrastructure that provides the services to a single organization, whether managed by internally or by a third party. Cloud which is hosted externally is termed as "externally hosted" private cloud and other hosted by third party are termed as "on premise" private cloud.

Community Cloud-It comprises sharing of computing infrastructure between organizations of identical community.

Hybrid Cloud-A hybrid cloud is a collection of private as well as public cloud options.) That remains unique entities but is bound together by standardized or proprietary technology.

IV. Cloud Computing Technologies

1. Microsoft Cloud Technologies

Microsoft is a foremost provider of cloud technologies and applications with results that matches with all type of business needs. It provides all type of services whether it is PaaS, IaaS or SaaS. If we talk about Infrastructure-as-a-Service Microsoft provides the windows server and system canter. And in case of Platform-as-a-Service it provide Windows Azure, with this you can easily build, host and scale applications in Microsoft Datacenter without up-front expenses just pay for what you use. Other PaaS services are SQLSERVER and VISUAL STUDIO. On the other way office365, share-point servers, dynamic CRM and exchange server are the Software-as-a-Services provided by Microsoft. With this we can say that Microsoft Cloud services are the complete package for your business.

2. Oracle Cloud Technologies

Oracle also provides the complete enterprise read public cloud solution including IaaS, PaaS and SaaS. With this you only need to concentrate on your business without worrying about IT management .oracle offers the following services

Database, it is available Database-as-a-Service along with accessing the Database in the Cloud directly through standard network connections, or as a Platform as a Service, with a complete development and deployment environment. You can avail its services as a single schema based service, or a virtual machine with a fully configured, running Oracle Database instance. To use oracle cloud database you just need to create an account with a valid email id and login with the provided credentials, you can enjoy this service for free for 30 days trial after that you can choose their given plans as per your need.

Oracle java cloud service as this service it gives you the application development and infrastructure and management tools ,you can develop J2EE standards JSP, JSF, Servlet, EJB, JPA,JAX – RS and JAX-WS applications .You can run popular frameworks like Spring , Hibernate and develop in your choice of cloud –enabled IDE such as Oracle JDeveloper, Eclipse and NetBeans . And last but not the least Web Logic Server as an application server.

Oracle mobile cloud –It is a simple enterprise mobile connectivity, it provides you easily named interfaces ,mobile APIs and build mobile apps for your enterprise systems. Mobile cloud provides you may more facilities such as mobile Apps, Notifications (email, SMS, voice) and data sync.

Oracle cloud document and oracle cloud storage –It provide you an easy and controlled cloud based file sharing and collaboration solution strong security. And oracle cloud storage facility offer you a reliable and secure data storage platform for storing and accessing data from any place connected to internet. Provide the features like backup, sharing, saving and distributing data between application and users without any difficulty.

Oracle cloud messaging-Oracle cloud messaging service enables infrastructure that make a communication link between software components with the facility of sending and receiving messages through single messaging API and create an active mechanize business workflow atmosphere.

Oracle cloud compute –with the help of oracle cloud compute we get the leverage infrastructure which provides us elastic compute capacity to address increasing business needs

3. Google Cloud Technologies

Google cloud also provides the services such as Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service. Google cloud enables developers to build, test and deploy applications on Google's highly scalable and secure infrastructure. As we know that Google has already provided infrastructure that allows Google to return billions of search results in milliseconds, provide storage for about 425 million Gmail users and serve 6 billion hours of YouTube video per month. Google has the ability to build, organize and operate a huge network of servers and fiber-optic cables .All this in aggregate makes Google the King of all cloud.

Google Apps Engine-with Apps Engine you can run your applications on a fully managed Platform-as-a-Service using built-In services. Here you can write applications in some of the most popular programming languages such as java, PHP and Python.

Compute Engine- with compute engine you can run large –scale workload on virtual machine hosted o Google's infrastructure .what you need is just choose a VM that fulfil your needs and take advantage of Google's performant, scalable, highly reliable and secure worldwide fiber network.

Cloud SQL-cloud SQL provides you the fully managed, relational My-SQL database to store and manage data. Google deal with the replication, patch management and database management to ensure availability and performance. My-SQL database deployed in the cloud without any difficulty.

Google BigQuery- it is the tool which provides the facility to analyze big data in cloud. It executes large datasets in seconds and it is very easy and scalable, BigQuery gives you real time clear cut picture about your data.

Google Prediction API- if you want to predict future trends using historical data use Goggle's machine learning algorithms to analyze data and predict upcoming results. You can Route messages, detect spam and recommend products for users with the help of Prediction API. Prediction API can be integrated with Apps Engine and the API is available with full libraries for several popular languages such as Python, .Net and JavaScript.

So there are many more services provided by Google cloud such as you can build online games and mobile apps on Google cloud platform. It also provides the storage space to store your data and share with others and many more facilities. There are some companies which are using Google cloud storage to meet their needs such as DNAnexus and Ubisoft.

V. Cloud Computing Security Threats

Cloud computing faces as much security threats as that are existing in the networks, intranets .these threats come in various forms. Cloud computing alliance did research in 2013 on cloud computing security threats and identified these threats.

- ➢ Traffic Hijacking
- ➢ Insecure Interface and APIs.
- ➢ Denial of Service.
- ➢ Malicious Insiders.
- ➢ Abuse of Cloud Services.
- ➢ Insufficient Due Diligence.
- ➢ Shared Technology Vulnerabilities
- ➢ Data Breaches
- ➢ Unknown Risk Profile
- ➢ Perimeter Security Model Broken
- ➢

VI. Cloud Security Issues

While cost and ease of use are the two main strong benefits of the cloud computing, there are some major alarming issues that need to be referenced when allowing moving critical application and sensitive data to public and shared cloud environment. The main aspect describing the achievement of any new computing technology is the height of security it provides whether the data located in the cloud is protected at that level that it can avoid any sort of security issue. So we must say that Security and privacy are the key challenges in the cloud computing. Here are some security issues, we have presented in this paper.

❖ Data confidentiality issue: Confidentiality is a set of rules or an agreement that bounds access or location restriction on certain types of information so in cloud data reside publically so Confidentiality refers to, customer's data and computation task are to be kept confidential from both cloud provider and other customers who is using the service. We must make sure that user's private or confidential information should not be accessed by anyone in the cloud computing system, including application, platform, CPU and physical memory. It is clear that user's confidential data is disclosed to service provider on the following situation only.

- Situation 1.The first situation where user's information may be disclosed when service provider knows where the user's private information resides in the cloud systems.
- Situation 2. The second situation where user's information may be disclosed when service provider has the authority to access and gather user's private information in the cloud systems.
- Situation 3.The third situation where user's information may be disclosed when service provider can figure out the meaning of user's information in the cloud systems.

These are the following situation due to, service provider can collect or get access user's information or data, if the service provider must know the place of the data in the cloud computing and have the authority to access users data. As we know that the current cloud computing consists of three layers Software layer, Platform layer, Infrastructure layer. Software layer provider the user interface for the user to use the services running on the cloud infrastructure. The platform layer provides the platform such as operation environment for software to run with the help of provided system resources. And the infrastructure layer provides the hardware resources for computing, storage and network. Although as the each service provider has its own software, platform and infrastructure layer with this when user uses the cloud application provided by service provider, it is mandatory for the user to use the platform as well as infrastructure provided by the service provider and therefore service provider is aware of, where the user's data is placed and the full accessibility to the data.

❖ Data availability issue – when keeping data at remote location which is owned by others, data owner may face the problem of system failure of the service provider. And if cloud stops working, data will not be available as the data depends on single service provider. Threats to data availability are flooding attacks causes deny of service and Direct /Indirect (DOS) attack. Cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system.

❖ Data integrity issue –as the word itself explains the "completeness" and "wholeness" of the data which is the basic and central needs of the information technology, As we know that integrity of data is important in the database equally integrity of data storage is important and necessary requirement in the cloud, it is the key factor that shaken the performance of the cloud. The data integrity proofs the validity, consistency and regularity of the data. It is the perfect method of writing of the data in a secure way the persistent data storage which can be reclaim or retrieved in the same layout as it was stored later. Therefore cloud storage is becoming popular for the outsourcing of day-to-day management of data .So integrity monitoring of the data in the cloud is also very important to escape all possibilities of data corruption and data crash. The cloud provider should provide surety to the user that integrity of their data is maintained in the cloud.

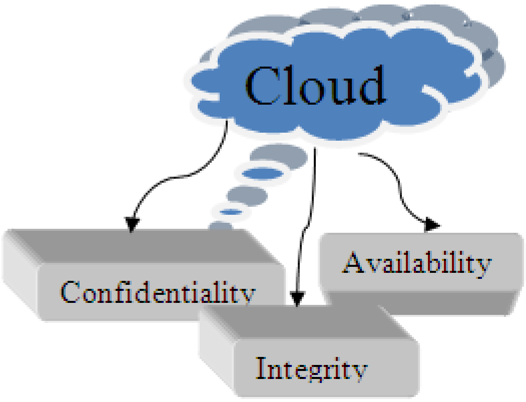

Fig: Basic security traits

❖ Data security issue-when we talk about data storage in the cloud computing or on premise application deployment model, the sensitive data of every enterprise continues to reside within the enterprise boundary and is focus to its physical, logical and personnel security and access control guidelines. Though in Software-as-a-Service model or public cloud the enterprise data is stored outside the enterprise boundary, by the CSP. So as a result, the CSP must agree to implement additional security checks to ensure data security and need to prevent breaches because of security vulnerabilities in the application or through malicious employees. These all above concern issues require to use a strong encryption techniques for the protection of the data because the some traditional encryption which have been used since, are not as powerful as we need. The data protection needs to be implemented in order to secure data from the following uncertainties.

❖ Trust issue- trust in the both conventional IT business and cloud computing need to be earned. Trust is also a major issue in cloud computing. Trust revolve around 'assurance 'and confidence that people, data, objects, information will perform or behave in projected way. Trust can be in between, human to human, machine to machine, human to machine or machine to human. Therefore in cloud computing when any user store their data on cloud storage, they must have trust to the cloud provider so that they don't scare to put their data on cloud, likewise we use Gmail server, yahoo server because we trust our provider. As we know that cloud is becoming popular, many people are using cloud but still people have some doubt in their confidential mind that their data might not be safe in the cloud like they don't put their account no, passport copy and other confidential information they might think that their information may be stolen or misused. Therefore cloud provider must have to come forward to tackle with the trust issue and build trust with the users so that more and more people will be able to take advantage of cloud computing without having any doubt.

❖ Data locality issue- in the data storage model of cloud computing environment the user the applications provided by the service provider and process their data but in this scenario the user does not have any knowledge about where their data is being stored, in many situations this can be a legal issue.

VII. Solution for Security Issues in Cloud Computing

- Scrutinize Support: when users store their data in the provided cloud they don't have the information where the data is stored. Therefore cloud service provider must provide audit tools to the users to examine regulate how there is stored, protected, used and verify policy implementation. But Scrutinizing of illegal activities is a difficult task because data for multiple users may be collocated. To solve this problems audit tools must be contractually committed with proof.
- Recovery facility: cloud provider must provide safe and helpful recovery facility, so in any situation if data is fragmented or lost because of any reason, data can be recovered so that continuity of data can be managed.
- Back up facility: natural disaster may harm or damage physical devices that may be the reason of data loss. Therefore to avoid this problem vendor must provide the backup of information, this facility gives a key assurance of service provided by service providers.
- Encryption algorithm: we that cloud service provider encrypt user's data using a strong encryption technique but in some circumstances encryption accidents can make data completely useless and on the other side encryption also complicates the availability of data. To solve this challenging problem cloud provider must provide proof that encryption technique were design and properly tested by knowledgeable and experience authority.
- Better Enterprise Infrastructure: Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber-attacks.

VIII. Conclusion

Cloud computing is the cost, time and performance effective technology. Of course the usage of cloud computing will surely will increase more in next few years. In this paper we have discussed and surveyed basic of cloud computing and security issues in the cloud computing. Some security issues are the key concern in the cloud computing. Especially privacy and integrity of data are the key concern security issues. In the cloud as data is stored publically and we really don't know where the data is being stored, we don't know the exact location of the data, due to this data stored in the cloud has a higher risk of being accessed by un- theorized person during storage as well as transmission.

References

i. *Sharma, Rajeev, and Bright Keswani. "STUDY& ANALYSIS OF CLOUD BASED ERP SERVICES."*

ii. *Juneja, Gurpreet K. "Use of Modeling Language to deploy applications in clouds."*

iii. *DHIWAR, KAMLESH KUMAR. "ASPECT OF CLOUD COMPUTING."*

iv. *Akintomide, O. A. "Cloud computing: The third revolution in IT." Library Progress (International) 33.1 (2013): 77-94.*

v. *Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing (draft)." NIST special publication 800.145 (2011): 7.*

vi. *Pearson, Siani, Yun Shen, and Miranda Mowbray. "A privacy manager for cloud computing." Cloud Computing. Springer Berlin Heidelberg, 2009. 90-106.*

vii. *T OGRAPH, B., and Y. RICHARD MORGENS. "Cloud computing."Communications of the ACM 51.7 (2008).*

viii. *Velte, Toby, Anthony Velte, and Robert Elsenpeter. Cloud computing, a practical approach. McGraw-Hill, Inc., 2009.*

ix. *Marinos, Alexandros, and Gerard Briscoe. "Community cloud computing."Cloud Computing. Springer Berlin Heidelberg, 2009. 472-484.*

x. *Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." Journal of internet services and applications 1.1 (2010): 7-18.*

xi. *Qian, Ling, et al. "Cloud computing: An overview." Cloud Computing. Springer Berlin Heidelberg, 2009. 626-631.*

xii. *Leavitt, Neal. "Is cloud computing really ready for prime time." Growth 27.5 (2009).*

xiii. *Voorsluys, William, James Broberg, and Rajkumar Buyya. "Introduction to cloud computing." Cloud Computing (2011): 1-41.*

xiv. *Wang, Lizhe, et al. "Cloud computing: a perspective study." New Generation Computing 28.2 (2010): 137-146.*

xv. *Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. "Towards trusted cloud computing." Proceedings of the 2009 conference on Hot topics in cloud computing. 2009.*

xvi. *Chen, Quan, and Qianni Deng. "Cloud computing and its key techniques."Journal of Computer Applications 29.9 (2009): 2565.*

Zhang, Liang-Jie, and Qun Zhou. "CCOA: Cloud computing open architecture."Web Services, 2009. ICWS 2009. IEEE International Conference on. Ieee, 2009.

xvii. *Iosup, Alexandru, et al. "Performance analysis of cloud computing services for many-tasks scientific computing." Parallel and Distributed Systems, IEEE Transactions on 22.6 (2011): 931-945.*

xviii. *Voas Jeffrey, and Jia Zhang. "Cloud computing: New wine or just a new bottle?" IT professional 11.2 (2009): 15-17.*

xix. *Piplode,k.singh."An Overview and Study of Security Issues & Challenges in Cloud Computing ".Volume 2, Issue 9, September 2012, ISSN: 2277 128X.*

xx. *L.chen."Using algebraic signatures to check data possession in cloud storage." Future Gener. Comput. Syst.29 (7): 1709-1715.*

xxi. *Sowparnika,R.Dheenadayalu"Improving data integrity on cloud storage services," IEEE Transactions on Knowledge and Data Engineering, Volume 23, no. 9, pp. 1432-1437, September, 2011.*

xxii. *Giuseppe, R.Burns, et al. "Remote data checking using provable data possession." ACM Trans. Inf. Syst. Secure.14 (1): 1-34.*

xxiii. *Martin, S. Schrittwieser, et al. Dark clouds on the horizon."using cloud storage as attack vector and online slack space". Proceedings of the 20th USENIX conference on Security. San Francisco, CA, USENIX Association.*

xxiv. *Subashini,V. Kavitha "A survey on security issues in service delivery models of cloud computing." Journal of Network and Computer Applications 34(1): 1-11.*

xxv. *H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393–398.*

xxvi. *Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments.Communications in Computer and Information Science; 2010;54:255–265.*

xxvii. *Fernandes, Diogo AB, et al. "Security issues in cloud environments: a survey."International Journal of Information Security (2013): 1-58.*

xxviii. Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." *International Journal of Computational Intelligence and Information Security* 3 (2012).

xxix. Sen, Santanu Kumar, and Sharmistha Dey. "An Investigation towards Security Threats for Cloud Computing.